

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-089737

(43)Date of publication of application : 15.04.1991

(51)Int.Cl.

H04L 9/06
H04L 9/14

(21)Application number : 01-217593

(71)Applicant : MOTOROLA INC

(22)Date of filing : 25.08.1989

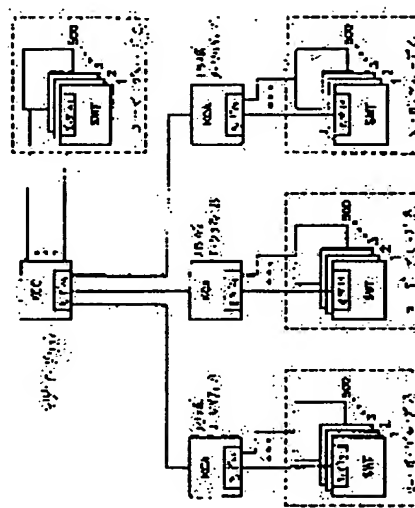
(72)Inventor : ROBERT IVAN FOSTER
ROBERT FREDERIC PFEIFER
THOMAS JAMES MIM JR

(54) HIERARCHICAL KEY MANAGEMENT SYSTEM

(57)Abstract:

PURPOSE: To establish secret protection between terminal users by providing the system with plural key permission authority means, corresponding to user groups and a terminal means groups and a key permission center means for applying authority to each of the key permission authority means and permitting direct secret protection communication between the terminals of different groups.

CONSTITUTION: A terminal group in the hierarchical key management system corresponds to one of user groups, and a large number of users can execute secrecy protective communication with other users by respective terminals SWT through a public exchange telephone network. The system has plural key permitting authorities(KCAs), and each KCA permits a user in a certain group to use a terminal for executing secrecy protective communication with another user in the same user group. The system has also key permission centers (KCCs), and each KCC is connected to plural KCAs to provide permission authority to each KCA and permit secret protection communication between different user groups. Consequently direct secrecy protection between terminal users can be established.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A) 平3-89737

⑬ Int. Cl.³

識別記号

庁内整理番号

⑭ 公開 平成3年(1991)4月15日

H 04 L 9/06
9/14

6914-5K H 04 L 9/02

Z

審査請求 未請求 請求項の数 10 (全9頁)

⑮ 発明の名称 階層型キー管理システム

⑯ 特 願 平1-217593

⑰ 出 願 平1(1989)8月25日

⑱ 発 明 者	ロバート・イワン・フ オスター	アメリカ合衆国アリゾナ州メサ、イースト・ヘイル・サー クル4023
⑲ 発 明 者	ロバート・フレデリッ ク・フェイファー	アメリカ合衆国アリゾナ州スコッツデイル、イースト・ア コマ・ドライブ5236
⑳ 発 明 者	トーマス・ジェーム ス・ミム・ジュニア	アメリカ合衆国アリゾナ州メサ、イースト・フェアフィー ルド5926
㉑ 出 願 人	モトローラ・インコー ポレーテッド	アメリカ合衆国イリノイ州シヤンパーグ、イースト・アル ゴンクイン・ロード1303
㉒ 代 理 人	弁理士 本城 雅則	外1名

明 細 書

1. 発明の名称

階層型キー管理システム

2. 特許請求の範囲

1. 複数のユーザの一部が交換回線網を経由して機密保護通信を行うことを可能にする階層型キー管理システムにおいて、前記階層型キー管理システムは：

前記ユーザの予め定めるユーザ・グループ；

共通のオーソリティによって予め許可されている前記各ユーザ；

前記交換回線網に接続され、前記交換回線網を経由して機密保護通信を行う端末手段；

端末手段のグループであって、各グループは前記ユーザのグループに対応し、第1端末手段が前記交換回線網を経由して第2端末手段と通信を行う前記端末手段のグループ；ならびに

前記第1および第2端末手段は、前記共通オーソリティに接続されることなく、前記交換回線網

を経由して機密保護通信を直接行うことを特徴とする階層型キー管理システム。

2. 前記共通オーソリティが：

ユーザ・グループの前記ユーザを許可する複数のキー許可オーソリティ手段であって、前記キー許可オーソリティ手段はユーザ・グループおよび端末手段グループに対応し、各キー許可オーソリティ手段は前記ユーザ・グループの他のユーザと直接機密保護通信を行うために前記端末手段を使用することを許可し、前記複数の各キー許可オーソリティ手段は前記対応するグループの前記端末手段に接続される前記複数のキー許可オーソリティ手段；および

前記複数の各キー保障オーソリティ手段に接続されたキー許可センタ手段であって、前記許可センタ手段は許可オーソリティを前記キー許可オーソリティ手段の各々に与え、異なったグループの端末手段の間で直接機密保護通信を認める前記キー許可センタ手段によって構成されることを特徴とする請求項1記載の階層型キー管理システム。

3. 個々のユーザに対応し前記端末手段に接続可能な機密保護動作装置手段をさらに有し、前記機密保護動作装置手段は前記端末手段に対して転送を行うため認証、符号化および復号化情報を格納するために動作することを特徴とする請求項2記載の階層型キー管理システム。

4. 前記機密保護動作装置手段は、前記端末手段にさらに接続され、前記端末手段が許可情報によって前記機密保護動作装置手段をプログラムすることを可能にすることを特徴とする請求項3記載の階層型キー管理システム。

5. 前記機密保護動作装置手段は前記端末手段にさらに接続され、前記端末手段が再発生した通信情報によって前記機密保護動作装置手段を繰返して再プログラムすることを可能にすることを特徴とする請求項4記載の階層型キー管理システム。

6. 前記ユーザ・グループのユーザは、サービスを行っていないユーザ・グループのキー許可認証手段の条件によって前記キー許可センタ手段に直接接続されることを特徴とする請求項2記載の

9. 前記機密保護動作装置に含まれる情報を前記端末によって検証し、前記ユーザが現在許可されていることを保証する段階をさらに有することを特徴とする請求項8記載の方法。

10. 複数のユーザが電話回線網を経由して機密保護通信を行うことを許可する階層型キー管理システムにおいて、前記階層型キー管理システムは：

前記ユーザの予め定めるユーザ・グループ；

各グループがユーザの前記グループに対応する端末手段のグループであって、前記各端末手段は前記電話回線網を経由して他のユーザとあらかじめ定めるユーザ数まで機密保護通信を行うことを可能にする前記端末手段のグループ；および

ユーザ・グループの前記ユーザが前記ユーザ・グループの他のユーザと機密保護通信を行うために前記端末手段を使用することを許可し、または異なったユーザ・グループのグループ間の機密保護通信を認めるキー許可手段によって構成されることを特徴とする階層型キー管理システム。

階層型キー管理システム。

7. 少なくとも2つの端末間で電話回線網を経由して機密保護通信を行い、前記各端末が共通のオーソリティから以前の許可を受け取る方法において、前記方法は：

前記2つの端末間で情報の転送を行うため電話回線網を経由する接続を完了する段階；

前記共通のオーソリティの符号化キーの下で前記2つの端末間で符号化キーを交換する段階；

端末に対して各々の転送およびキー対を決定し、前記2つの接続された端末間での機密保護通信を可能にする段階；および

引き続き行われる機密保護通信のため各端末に特有の第2の変更した符号化／復号化キー対を保存する段階によって構成されることを特徴とする方法。

8. 機密保護動作装置を前記端末に挿入し、対応する端末の各ユーザが機密保護通信を行なえることを許可する段階をさらに有することを特徴とする請求項7記載の方法。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は、機密保護機能のある電気通信システムに関し、さらに詳しくは、ユーザの認可および認証を行う権限を有する代表者を支援する拡張性のある階層型キー管理システムに関する。

(従来の技術)

代表的なキー管理システムは、1986年3月25日J. エバーハート等に付与された米国特許第4,578,531号に示されている。この発明は、機密保護機能のある複数の各端末に接続されたキー分配システムを開示する。機密保護のあるデータ伝送を希望する場合、各端末はキー分配センタとの通信を確立しなくてはならない。これによりキー分配センタは、端末の資格審査を行い、必要な機密保護の分析を実行する。

(発明が解決しようとする課題)

このシステムの欠点は、キー分配センタが、全ての2つの端末間のそれぞれの機密保護通信に関与しなくてはならないことである。端末は、自己

の情報の機密保護バケットをキー分配センタを経由してのみ交換する。各端末は、検証のために許可情報をキー分配センタに送り、その結果得られる情報をキー分配センタから受信しなければならない。このような多重通信は効率的でない。

さらに、上述のシステムは、機密保護が階層的になっていない。全ての重要なキー・データがセンタに集中しているため、もしキー分配センタの機密保護が危険にさらされると、各ユーザの機密保護もまた危険にさらされる。

したがって本発明の目的は、端末ユーザ間で直接機密保護を確立することのできる階層型のキー分配システムを提供することにある。

(課題を解決するための手段)

本発明の目的を達成する場合の新規な階層型キー分配システムを示す。

階層型キー管理システムは、複数のユーザに公衆交換電話回線網を経由する機密保護通信を許可する。階層型キー管理システムは、ユーザを限定したユーザ・グループに割当てて。

C)はこのシステムの中核をなすオーソリティである。KCCは、キーボード、表示端末、ハードディスク、バックアップ用テープ・ストリマ、プリンタおよび通信用インタフェイス端末(network interface terminal : NIT)を有する専用の特別の目的に供するコンピュータ・システムで構成することが可能である。NITは、以下で説明する。

各KCAおよびKCCは、公衆交換電話回線網を経由してKCAおよびKCCの高速度の電話による接続を行うモデムを有する。他の通信伝達手段を使用することも可能である。3つのKCAは、第1図に示す地域オーソリティA、地域オーソリティB、地域オーソリティCである。しかし、KCCに4つ以上のKCAを接続することも可能である。

各KCAはまた、キーボード、表示端末、ハード・ディスク、バックアップ用テープ・ストリマ、プリンタおよび通信用インタフェイス端末を有するコンピュータ・システムで構成される。各

階層型キー管理システムは、端末群を含む。各端末群はユーザの1つのグループに対応する。各端末によって、多数のユーザが公衆交換電話回線網を経由して他のユーザと機密保護通信を行うことが可能になる。

階層型キー管理システムは、複数のキー許可オーソリティ(key certification authority : KCA)を有している。このキー許可オーソリティは、ユーザ・グループのユーザが上記のユーザ・グループの他のユーザと機密保護通信を行うために端末を使用することを許可する。

階層型キー管理システムは、またキー許可センタを有している。この各キー許可センタは複数の各キー許可オーソリティに接続される。キー許可センタは許可オーソリティを各キー許可オーソリティに与え、異なるユーザ・グループ間での機密保護通信を認める手段を提供する。

(実施例)

第1図は、キー管理システムの階層を示す。キー許可センタ(key certification center : KCC

地域オーソリティすなわちKCAは、500以上のユーザを取り扱うことが可能であるが、一般的に最高500のユーザ間で機密保護通信を提供する。例えば、地域オーソリティAは、ユーザ・グループAのユーザ間で機密保護通信を可能にする。各ユーザのグループA、B、およびCは、典型的には最高500の機密保護線路端末(secure wireline terminal : SWT)によって構成される。ユーザとは、ユーザ・グループ内で1つ以上のSWTを使用することを許可された個人である。

各SWTは、トラフィック・キーの機密保護交換用の非対称キーを発生する。SWTは、端末のアクセスおよびユーザ保障用の機密保護作動装置(security activation device : SAD)を有する。このSADは、最初にKCAによってプログラムされ、続いてSWTによって再プログラムされる物理的なキーである。このSADは、機密保護通信およびユーザの認定を可能にするためにSWTのコンセントに挿入される。

このSWTは、各ユーザ用の独特で非対称な一

対の符号化／復号化キーを発生する。この非対称な一対のキーは、地域オーソリティ(KCA)によって許可される。2つ以上のKCAを有する大きな通信システムの場合、あるユーザ・グループに属するユーザは、他のユーザ・グループのユーザとの通話を希望する可能性がある。この場合、グループ間で通話を行うユーザは、共通するKCCに登録されたKCAによって許可されなくてはならない。

もしユーザの地域オーソリティ(KCA)が一時的にサービスを行っていない場合、KCCはサービスを行っていない全てのKCAをバックアップすることができる。これは、サービスを行っていないKCAのバックアップ・テープをKCCにロードすることによって行われる。

最初に、機密保護通信のユーザは、その地域オーソリティ(KCA)によってシードSAD(seed SAD)、および対応するパスワードが発行される。このシードSADは、第1すなわち最初のSADであることから自分の名前を得、その

SADから個々のユーザに関する機密保護情報が発生される。このシードSADは、ユーザの識別に関するデータおよび許可に必要な特別コードを有する。

ユーザは、SWTに自分のSADを挿入することによって許可を受けることが可能である。次に、ユーザは自分の地域オーソリティであるKCAに通話を試みる場合、パスワードを入力する。このSADおよびパスワードを使用して、ユーザは最大8つのSWTで許可を受けることが可能である。さらに、最高8名のユーザが個々のSWTで許可を受けることが可能である。SWT1台当たりのユーザ数およびユーザ1名当たりのSWT数は典型的には8に設定されるが、SWT1台当たりのユーザ数およびユーザ1名当たりのSWT数をより多くする柔軟性が与えられている。

ユーザが一度特定のSWTで許可されると、このユーザは、同じ地域オーソリティ内の他のユーザと、または自動化されたキー発信および2つの端末を連結して行われる分配プロセスを介して、

共通のKCCを共有する他のユーザと機密保護通話することが可能である。すなわち、ユーザ・グループAに属するユーザは同グループに属する他のユーザと通話が可能であり、またはグループBに属するユーザ、またはグループCに属するユーザと通話可能でありまたその逆も可能である。SWTのユーザが一度許可を受けると、このユーザは、公衆交換電話回線網(public switched telephone network: PSTN)または他の回線を介して通常の通話が可能である。この通話が機密保護通話であるべきであると決定されると、SWT上の機密保護押しボタンが押される。特定の通話における2つのSWTは許可データを交換し、トラフィック・キーを発生しこれを交換する。この時点で機密保護通信が確立する。この同期および機密保護プロセスの一部として、他のパーティの識別および接続の機密保護レベルのような認証情報がSWT上に表示される。

ユーザの許可の時点で、KCAは終期コードを許可されているユーザのSADまたはキーに付加

する。このユーザのSADの終期に先立ち、このユーザは自分のSADを再許可するように告知される。再許可のためには、ユーザは自分のパスワードおよびSADを使用して地域KCAを呼ぶ。再許可の間、端末はKCAによって許可される新規の非対称符号化／復号化キーの一対とユーザのSADに付加され、格納される新しい終期を発生する。もしユーザが終期日に先立ってKCAによる再許可を行なわなかった場合、SWTはこのユーザのシステムへのアクセスを自動的に拒絶する。

オーソリティはこのキー管理システム全体を委任されている。KCCおよびKCAは各ユーザまたはSWTの個人用キーを持たない。従って、もしKCAまたはKCCのいずれかが1つが危険にさらされる場合でも、キー管理システム内の全てのユーザが危険にさらされることはない。しかし、KCCまたはKCAが危険にさらされていると、誤った許可を与える可能性がある。

オーソリティの代表権は、KCAがKCCにオーソリティとして登録されるプロセスを通して確

立される。このことは、PSTNによる機密保護プロセスを使用して行われる。一度KCAがKCCに登録されると、KCAは個々のユーザの許可プロセスの一部として登録バケットを発行することができる。これらの登録バケットによって、ユーザは他の地域オーソリティ・グループ（ユーザ・グループA、BまたはC）のユーザと機密的に通信をすることができる。

KCAは、新規の非対称通信領域キーを許可し、総括的な承認されていないキー情報を受信するため、規則的な間隔でKCCに対して再許可プロセスを実行する必要がある。KCAとKCCとの間で発生するこの処理は、メッセージの内容を除き、SWTとKCAとの間で行われる許可処理と同様である。

KCCは、総括的な承認されていないキーの一覧（unauthorized key list : UKL）を保持し分配する。このUKLの分配は、システムの階層を介して行われる。KCAは、これらの各SWTユーザからUKLを受信する。ロックアウト・バ

ケット（Lockout packet）であるこのデータはKCCに送信され、グローバルUKLを更新する。このグローバルUKLは、次にKCAを介して各SWTに分配される。UKL上でのユーザに対する機密保護期間はSWTによって自動的に防止される。もしこの構成にKCCが設けられていない場合、UKLはKCA中に格納される。

KCAによってシードSADが作られた時点からKCAがゼロになる（クリアされるかリセットされる）迄、すなわち無くなるか満了する迄、キー管理システムは該当するSADの使用を監視し、修正しかつこれに対する責任を負う。KCAによって一度ユーザが許可されると、2つのSWT間に機密保護通信伝送路を確立するために端末から端末間のみの通信が必要となる。これらの通信によって、SWT間に機密保護チャンネルが確立される。ユーザが自分のSWTの機密保護押しボタンを押した場合、一連のメッセージがSWT間で交換される。この交換される情報の幾つかは、SWTのモデムのチャンネル特性を示す。

第2図は、SWTのユーザ1AとSWTのユーザ5Aとの間の機密保護通話を示す。SWTのユーザ1Aと5Aは、同一の承認を行うオーソリティ、すなわち、第2図に示すKCA Aによって許可されるものとして示される。以下の説明は、SWT 1Aと5AがそれらのSAD（機密保護実行装置）キーを以前に許可している仮定している。このことは、SWT 1Aおよび5AをKCA Aに接続する線によって示され、かつ許可されたSADキーによって示される。それ以前の時点で、SWT 1Aと5Aは、いずれもこの許可プロセスを実行している。

SWT 1Aおよび5Aは電話回線を介して予め接続を確立している。この時点で、ユーザはSWT 1Aの機密保護押しボタンを押す。これによって、PSTNを経由して自動メッセージ交換が開始され、その結果、SWT 1Aと5Aとの間に機密保護のされた2400ボーの伝送路が確立される。2400ボーの伝送路は1例である。確立されたデータ伝送路は、いずれのデータ・レ

ートであってもSWTによって実行される。

次の第1表は、以下で使用する種々の符号化および復号化ベクトルの略語リストである。

第1表

Ex	ユーザの符号化ベクトル
Dx	ユーザの復号化ベクトル
Exa	キーのオーソリティ符号化ベクトル
Dxa	キーのオーソリティ復号化ベクトル
Eax	キーのオーソリティ許可符号化ベクトル
Dax	キーのオーソリティ許可復号化ベクトル
Ec	キーの許可符号化ベクトル
Dc	キーの許可復号化ベクトル
Exts	ユーザの許可符号化ベクトル
Dxts	ユーザの許可復号化ベクトル

各ユーザは、自分の許可されたSADキーをそ

それぞれのSWTに挿入する。最初に、2つのSWTはアクセス/領域メッセージを交換する。これらのメッセージは、1つのオーソリティID(KCAの識別)、バージョン番号、Dax用終期データ、中央ID(KCCの識別)、バージョン番号、Dc用終期データ、端末のタイプおよび端末のシリアル番号を有する。両SWTは送信されたメッセージを検査し、共通の非対称通信領域キー、DaxまたはDcのいずれかと一致させようとする。両SADがKCAによって許可されるので、一致が起こる。

次に、各SWTは他方に認証バケット・メッセージ(Authentication Packet message)を送る。この認証バケット・メッセージには以下の情報が入っている。すなわち、これらは、ユーザのIDサイン(ID signature: IDS)、ユーザのID、SADのシリアル番号(SAD serial number: SSN)、アクセス情報、端末のシリアル番号(Terminal serial number: TSN)、およびユーザの許可された非対称キーExtである。

またキーをかけるのに使用されてきた。

最後に、クリプト同期(Crypto Sync: CS)メッセージ・バケットが各SWTによって発生される。SWT 1Aおよび5Aは、次にPSTNを経由してクリプト同期(CS)メッセージ・バケットを交換する。各SWTは、次に他のSWTから受信したクリプト同期メッセージを処理する。クリプト同期メッセージは受信Kgによって処理され、クリプト同期を得る。クリプト同期が達成されると、各SWTは自分のユーザに、機密保護伝送路が適切なボー・レートで確立されたことを知らせる。

もし2つのSWT間の通信が2400ボー・レートで行われる場合、上記の機密保護処理は約10秒を要する。誤りの影響を最小にするため、データ交換に対して順方向エラー修正(forward error correction)が使用される。

第3図では、SWTユーザ1AからSWTユーザ7Bへの機密保護通話を説明する。SWTユーザ1AはKCA Aによって許可されている。S

る。

各SWTは他方の認証バケット・メッセージを受信し、これを共通する領域キーDaxを用いて復号する。その結果、各SWTは他方の非対称キーExtを引き出す。他方のユーザのIDがSWT上に表示される。表示されたIDは、また2人のユーザの有する最低位の共通の等級を示す。もしアクセス情報に重要な不一致が発見されると、通話は終了する。

次に、各SWTは1つのランダム成分(Random Component: RC)の2つの複製コピーを発生し、これらはKgのキーイングに使用される。RCのコピーの1つが地域送信Kgに転送される。RCの他のコピーは他方のユーザExtを用いて符号化される。各SWTは、この時点でランダム成分メッセージ・バケットを他方のユーザに送信し、これは他方のユーザExtで符号化される。各SWTが他方のランダム成分メッセージ・バケットを受信すると、Dxtを用いてそのバケットを復号化する。ランダム成分は受信Kgのキーであり、

WTユーザ7Bは、あらかじめKCA Bによって許可されている。これは、SWT 1AとKCA Aとの間およびSWT 7BとKCA Bとの間の破線によってそれぞれ示される。KCA AおよびKCA Bはキー許可センタ(KCC)Xによって予め許可されている。前述のように、SWT 1AおよびSWT 7Bは非機密保護の状態でPSTNを介して相互に接続される。SWT 1Aのユーザは、機密保護押しボタンを押し、その結果、アクセス/領域メッセージ・バケットがSWT 1Aと7Bと間に送信される。これらのアクセス/領域メッセージはKCC IDおよびバージョンを有しているので、アクセス/領域メッセージ・バケットは一致する。異なったKCCに属するSWT間の機密保護通話は、このシステムの下では認められていない。

KCAではなくKCCの同一性によって一致が判定されるので、SWT間の次のメッセージ送信は、上述の共通なKCAの場合とは異なったものになる。この場合のSWT間の次のメッセージ・

パケットの送信は登録パケット (Registration Packet) と呼ばれる。この登録パケットは以下の情報で構成される。すなわちこれらは、承認を行うKCAの非対象領域キー (Dax)、KCAのIDおよび各KCAに関するアクセス情報である。登録パケット全体はKCCの領域キーEcを使用して復号化される。各SWTは他の登録パケットを受信し、共通の領域キーDcを用いて復号化する。結果として、各SWTは他方の非対象領域キーDaxを抽出する。各SWTが他方のKCCの同一性およびバージョンが正しく一致すると判定した場合、上述のように機密保護プロセスが行われる。もしKCCのIDおよびバージョンが一致しない場合、機密保護通話は終了する。

登録パケット・メッセージが正しく復号化された後、認証メッセージ・パケットがSWT 1Aと7Bとの間で交換される。認証パケット・メッセージに対する処理が、共通のKCAの場合に対して、上述したように行われる。次に、ランダム成分メッセージ・パケットがSWT 1Aと7B

との間で交換される。再び、この処理も上述のように共通のKCAに対して行われる。最後に、クリプト同期メッセージ・パケットがSWT 1Aと7Bとの間で交換され、上述のように処理される。

異なったKCA領域であるが、共通のKCC領域にあるSWT間での機密保護通話を行う場合、通信レートを2400ボーと仮定すると、2つのSWT間での機密保護通話を確立するのに要する時間は約15秒である。

第1図に示すように、KCAがサービスを行っていない場合、該当するKCAを許可しているKCCは、KCAのバックアップとして動作可能である。ユーザ・グループ・バックアップは、ユーザ・グループA、BおよびCのようないずれのユーザ・グループにも提供される。これを行うため、サービスを行っていないKCAのバックアップ・テープがKCCにロードされる。このような構成でユーザを許可するため、KCCはKCAとして動作する。

KCAに対する最初の許可は、SWT上のSADに対するKCAの最初の許可と同じ方法で行われる。KCAに対する最初の許可のため、この特定のKCAに対してパスワードおよびシードSADを使用して機密保護伝送路が作られる。例えば、KCA Aまたは地域オーソリティAは中央オーソリティKCCに機密保護伝送路を確立する。機密保護伝送路が確立されると、KCAは許可情報パケットを送る。このパケットは、オーソリティの識別サイン (IDS)、端末のシリアル番号 (TSN)、Exa、DaxおよびSADのシリアル番号 (SSN) を含む。

KCCは、ユーザを許可する場合にKCAがKCCのために動作することを保障する登録パケットを使用してKCAに回答する。さらに、KCCはKCAにロックアウト・パケットを送るが、これは認定されていないキーの一覧およびグローバルな復号化キーDcである。登録パケットは新規に発生した非対称領域キーを有し、これらはKCCのEcを使用して符号化される。この登録パケッ

トはまたKCAの識別およびアクセス/クリアランス情報を有する。

特定のKCA非対称領域キーの認証期間が終了した場合、KCAは新規のキーをKCCで再許可する。再許可のプロセスは、あらかじめ設定された許可期間がまだ終了していないならば、グローバルな非対称領域キーDcがKCCによって送られない点を除き、本質的に最初の許可プロセスと同様である。

KCAによるユーザの許可後、このユーザを許可した特定のSWTはSADをカバーする成分を発生し、これはランダムに発生され、SADをカバーする成分によって符号化またはカバーされるアクセス領域メッセージをSWTの不揮発性メモリに記憶する。次に、このSWTは認証パケット、登録パケット、TSN (端末のシリアル番号) およびSADのカバー成分を格納する。このSWTはまた認定されていないキーの一覧 (UKL)、および同じSADカバー成分でカバーされる復号化ベクトルDcおよびDxtを格納する。使用毎

に、SADカバー成分は更新される。

第4図は、KCCまたはKCAのブロック図を示す。各KCAおよびKCCはコンピュータ制御のシステムによって構成することが可能である。このコンピュータ制御システムはCPU、ハードディスク、バックアップ・テープ装置、プリンタ、キーボード、表示装置、および通信用インターフェイス端末(NIT)によって構成される。このNITは、KCCまたはKCAにインターフェイスするための特別の機密保護線路端末である。このNITは、KCAの場合ユーザのモデムの全てに接続され、KCCの場合KCAに接続されるモデムを有する。

第4図に示す制御コンソールは、表示装置、キーボード、CPU、ハード・ディスク、バックアップ・テープ装置によって構成される。

NITは、ユーザとKCAとの間、またはKCAとKCCとの間でデータを高速転送する。NITはまた、ユーザとバックアップ・モードにおいてKCAとして動作するKCCとの間で高速通信

を直接行う。

各NITおよびSWTはモデムを有する。これらのモデムは、2400ないし9600ボーのような高速でデータを送る能力を有するが、これらの速度に制限されるものではない。

キーボードはCPUに対してデータ入力を行う。表示装置はCPUからの映像出力を行う。プリンタはCPU出力のハード・コピーによる映像表示を行う。ディスクは、SWTに関連する全てのオペレーティング・ソフトウェアおよびデータ・ベースを格納し、KCCの場合は、KCAに関する情報を格納する。バックアップ・テープ装置はサービスを行っていないKCCにKCA情報をロードし、その結果、KCCはKCAの機能を果たすることができる。さらに、バックアップ・テープ装置は、KCAまたはKCCがサービスを行っていない場合、システムを再ロードする。

本発明の好適な実施例が図示され、この実施例が詳細に述べられたが、本発明の精神または添付の請求項の範囲から逸脱することなく、種々の変

形が行われることは、当業者にとって容易であることは明らかである。

4. 図面の簡単な説明

第1図は、本発明の動作原理を実現するキー分配システムを示すブロック図である。

第2図は、同じ許可オーソリティによって提供される2つの機密保護線路端末間で機密保護通話を行うブロック図である。

第3図は、異なった許可オーソリティによって提供されるが同じキー許可センタである2つの機密保護線路端末間で機密保護通話を行うブロック図である。

第4図は、キー許可センタとキー許可オーソリティのブロック図である。

KCC・・・キー許可センタ、KCA・・・キー許可オーソリティ、SWT・・・機密保護線路端末、SAD・・・機密保護作動装置、PSTN・・・公衆交換電話回線網

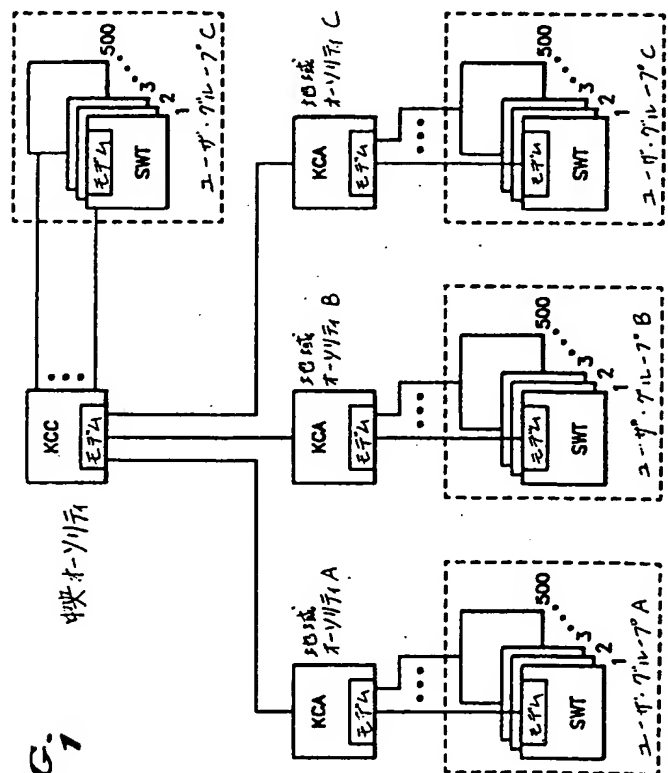


FIG. 1

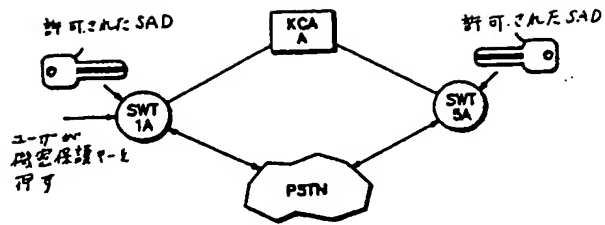


FIG. 2

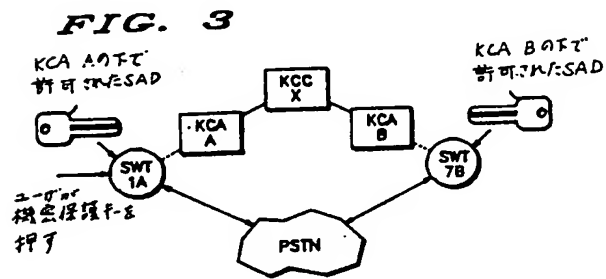


FIG. 3

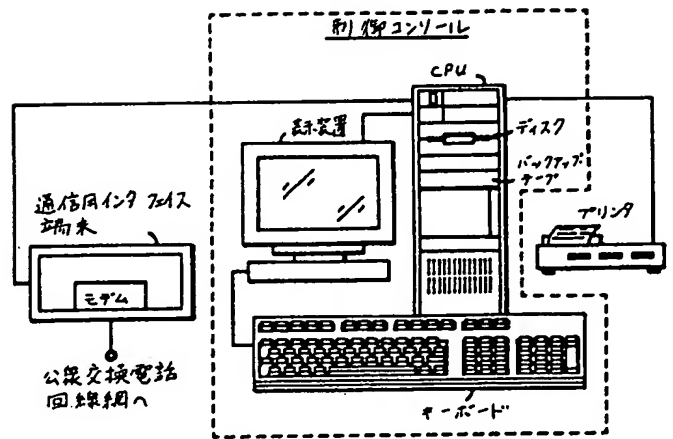


FIG. 4